[2345/45]

Method and Device For Loading Input Data into a Program When Performing an Authentication

Field of the Invention

The present invention relates generally to a method for loading input data into a program when performing an authentication, and, in particular, to a method for loading input data into a program when performing an authentication between electronic cash cards and a security module.

Related Technology

Various prior methods are used for electronic cash cards in a plurality of variants, with devices being based on, among other things, chip circuits as purportedly referred to by European Patent Application Number 0 616 429.

Related methods may be described, for example, in ETSI D/EN/TE 090114, Terminal Equipment (TE) Requirements for IC Cards and Terminals for Telecommunication Use, Part 4 - Payment Methods, version 4, of February 7, 1992, and in the European Patent Application Number 0 605 070.

In addition to phone cards, which have a defined initial credit balance as a payment means for card-operated phones, "electronic cash cards", which work according to the same principle, are gaining in significance as a means for paying limited amounts. In "pay with chip card" applications, a card reader module having a security module SM for verifying the card and the balance amount are integrated in the automatic machine.

European Patent Application Number 0 605 070 further purportedly refers to a method for transferring credit and debit amounts to and from chip cards, memory locations of a chip card having overwrite capability being divided into at least two memory areas, one of these having

a "debit function", thus acting as an "electronic purse" similarly to a phone card, and the other having a "credit function" along the lines of a credit card. To replenish the "electronic purse", provision is made for cash amounts to be transferred between the areas under the secured conditions that are typical for credit cards.

To both avoid the danger of unauthorized access to the automatic teller machines and their permanently installed security modules, as well as eliminate the need for dedicated lines which are specially protected and, thus, expensive for the operator, in a method described in PCT Patent Application Number 95114, prior to any cash transaction, the operator of the automatic cash machine inserts a security module having chip card functions into the automatic cash machine. During each cash transaction that involves a cardholder inserting his or her electronic cash card into an automatic cash machine, data areas of the chip card are first read out to permit a plausibility check and to verify the remaining credit balance. Subsequently, an authentication is performed using the security module and a single or multiple acceptance decision is made. Finally, the cash amount due or input is either debited to the cardholder's chip card with the aid of a security function, or added to a summing counter for cash amounts in the security module. Following the cash transactions, the counter content of the security module having chip card functions is transferred to a clearinghouse.

Summary of the Invention

An exemplary embodiment and/or exemplary method of the present invention is directed to enhancing the security of automatic cash machines for the electronic cash cards to prevent unauthorized manipulation and malfunctions.

~~Another exemplary embodiment and/or exemplary method of the present invention is directed~~ to loading input data into an algorithm ~~or a program~~ when performing a cash transaction ~~authentication between an electronic cash chip card and a security module~~.

Sub C1

Brief Description of the Drawings

Fig. 1 shows a block diagram of an exemplary method and/or embodiment according to the present invention.

Fig. 2 shows a block diagram of another exemplary method and/or embodiment according to the present invention.

add Out

Detailed Description

Fig. 1 shows a block diagram of an exemplary method according to the present invention for loading input data into a program when performing a cash transaction authentication between an electronic cash chip card and a security module, the chip card including a stored credit balance. As shown in block 102, a cash amount requested, preferably input by the cardholder, is debited from an electronic cash ship card using a security function. The requested cash amount is added and stored in a cash amount summing counter of a security module, as shown in block 104. Then, as shown in block 106, input data is subdivided into a plurality of data blocks. According to the present invention, the data blocks are loaded into a linear-feedback shift register for performing the program, the linear-feedback shift register having at least one nonlinear function cryptographically enhanced using at least one downstream counter, as shown in block 110. Lastly, as shown in block 112, the at least one additional feedback is switched off after a predefined number of clock pulses.

Fig. 2 shows a block diagram of an exemplary device 120 according to the present invention for loading input data into a program when performing an authentication using a cryptographic MAC function. The device 120 shown includes a first counter 122. The device 120 further includes a first linear-feedback shift register 124 which may have a nonlinear feed-forward function for reading off from the first linear-feedback shift register 124 and for influencing an output of the first linear-feedback shift register 124 using the first counter 122. The device 120 further includes at least one second counter 126 for performing a program associated with the present invention, the at least one second counter 126 being connected downstream, that is, after, the first linear-feedback shift register 124. The device 120 further includes at least one additional non-linear feedback shift register 128 for cryptographically enhancing the device 120, the at least one additional non-linear feedback shift register 128 being disconnectable from the device 120. In this exemplary device 120, the first counter 122 and/or the at least one second counter 126 may be subdivided or reduced.

Authentication algorithms may be used to enable reliable identification. Often entering into the authentication methods, besides the identity of a chip card, a person, and/or a security module SM, are other data, which have to be verified. An authentication method can be applied, for example, to non-secret card data D, together with a secret key K, and a random number Z. For the sake of security when working with electronic cash cards, separate security functions may be used for debiting and crediting, and each of these security functions may be retrieved using a cryptographic checksum.

add 105

Exemplary methods of the present invention may enable the debit and credit transactions to be carried out using a cryptographic token, where it is required that the authentication and cryptographic checksum process are performed on the counter content using a challenge/response method. A single challenge/response method can then be applied, whereby only one random number is provided by the security module SM and only one response is calculated by the chip card, to verify both the identity (authentication) as well as the internal counter content with respect to the security module SM.

Sub 01

This may be achieved with the variable input data, such as the counter content and the random number, being initially processed internally using "keyed hash functions," that is, MAC functions. In the process, the card-specific secret key of the chip card is used as the key. The two tokens extracted from the counter content and the random number may then be linked together, for example, (in a perhaps cryptographically unsecured way) by XOR or by using a linear-feedback shift register, and then may be output, with their integrity being protected, using a cryptographic function that is sufficiently powerful.

chipcard balance

This exemplary method of the present invention provides that the keyed hash functions, which are only used internally, do not have to meet any particularly high requirements with regard to their security, and relatively simple functions can be used since the results of these functions do not leave the chip card. Nevertheless, data manipulation may be effectively prevented with this exemplary method.

A further exemplary method and/or exemplary embodiment of the present invention may

~~assume that a~~ linear-feedback shift register (LFSR) having an additional nonlinear function and downstream counters is used. Exemplary steps and features may include that:

additional feedback circuits are switched into the linear-feedback shift register LFSR following the downstream counters;

input data, composed of the non-secret card data D and the secret key K, are read into the linear-feedback shift register LFSR, while both the feedback of the linear-feedback shift register LFSR, as well as the additional feedback(s) are active;

a certain number of clock pulses is processed without additional input data being read in;

input data made up of the random number R are read in while both the feedback of the LFSR and the additional feedback(s) are active;

the additional feedback circuits are switched off, and the counters are reset, if necessary; and/or

a certain number of clock pulses, for example, a third number of pulses of the clock, is processed, and, during these pulses, output bits are generated according to the current counter settings.

Abstract

A method for enhancing data security when chip cards are used for payment transactions and input data are loaded into an algorithm when performing an authentication. The security of the debit and credit data is enhanced by subdividing the data blocks and by switching an additional feedback on and off following the downstream counters at preselected clock pulse times. The method is applicable to all authentication processes in conjunction with chip cards.